UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ORIGINAL

- x

UNITED STATES OF AMERICA

-v.-

BEHZAD MESRI,
a/k/a "Skote Vahshat,"

Defendant.

SEALED INDICTMENT

17 Cr. _____

17 CRIM 689

- x

COUNT ONE
(Computer Fraud - Unauthorized Access to a Protected Computer)

The Grand Jury charges:

RELEVANT PERSONS AND ENTITIES

1. At all times relevant to this Indictment, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, was an Iran-based computer hacker. MESRI was a self-professed expert in computer hacking techniques, and had worked on behalf of the Iranian military to conduct computer network attacks that targeted military systems, nuclear software systems, and Israeli infrastructure. At certain times, MESRI was a member of an Iran-based hacking group called the Turk Black Hat Security team. As a member of that group, MESRI conducted hundreds of website defacements using the online hacker pseudonym "Skote Vahshat" against websites in the United States and elsewhere around the world.

2. At all times relevant to this Indictment, Home Box Office, Inc. ("HBO") was a media and entertainment company, headquartered in New York, New York. At all relevant times, HBO produced and broadcasted premium original television programming, which had substantial value and created significant revenue for HBO.

MESRI'S HACK AND EXTORTION OF HBO

3. From at least in or about May 2017 through at least in or about August 2017, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, orchestrated a scheme to obtain unauthorized access to HBO's computer systems, steal proprietary data from those systems, and then attempt to extort HBO for $6 million worth of Bitcoin, a form of digital currency.

4. Starting in at least in or about May 2017, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, conducted online reconnaissance of HBO's computer networks and employees. Among other things, MESRI searched for access points to the network where employees and other authorized users could remotely access HBO's computer systems.

5. Between at least in or about May 2017 and in or about July 2017, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, successfully compromised multiple user accounts belonging to HBO employees and other authorized users, and used those accounts to

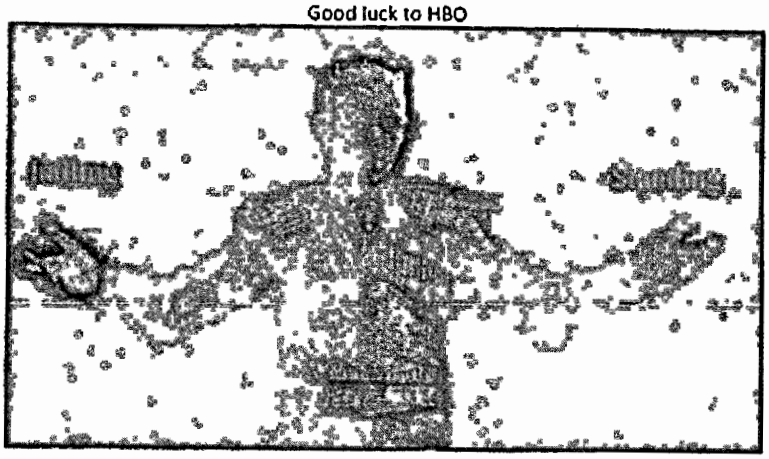
repeatedly obtain unauthorized access to HBO's computer servers. Over the course of several months, MESRI used that unauthorized access to steal confidential and proprietary information belonging to HBO which he then exfiltrated to computer servers under his control. Through the course of the intrusions into HBO's systems, MESRI was responsible for stealing confidential and proprietary data belonging to HBO, including, but not limited to: (a) confidential video files containing unaired episodes of original HBO television programs, including episodes of Ballers, Barry, Room 104, Curb Your Enthusiasm, and The Deuce; (b) scripts and plot summaries for unaired programming, including but not limited to episodes of Game of Thrones; (c) confidential cast and crew contact lists; (d) e-mails belonging to at least one HBO employee; (e) financial documents; and (f) online credentials for HBO social media accounts (collectively, the "Stolen Data").

6. Between on or about July 23, 2017, and on or about July 29, 2017, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, commenced the extortion phase of the scheme by transmitting or aiding and abetting the transmission of the following e-mail messages, each of which were sent to multiple HBO executives, employees, and other representatives, including to individuals located in the Southern District of New York:

a. On July 23, 2017, an anonymous e-mail was sent to HBO personnel that stated, in sum and substance, and among other things, that the sender had hacked into HBO's computer system. The e-mail stated, among other things, "Hi to All losers! Yes it's true! HBO is hacked! ... Beware of heart Attack!!!" The e-mail further stated, in substance and in part, that the sender had stolen approximately "1.5 [t]erabyte[s] of [HBO's] precious data." The e-mail also provided evidence that the hacker had successfully stolen proprietary data from HBO's computer servers.

b. Later that day, another anonymous e-mail was sent to HBO personnel that stated, in part, that "I have the honor to inform you ... that we successfully breached into your huge network[,]" that "in a complicated cyber operation, infiltration into your network [was] accomplished and we obtained most valuable information. (1.5 Terabyte)[,]" and that "...HBO was on[e] of our difficult targets to deal with but we succeeded." The e-mail included a threat to publicly release the Stolen Data unless HBO paid a "non-negotiable" ransom of approximately $5.5 million dollars' worth of Bitcoin. In that e-mail, the sender further claimed, in substance and in part, that the sender had obtained full scripts and final video files; "precious data" for the HBO shows Ballers, Barry, Insecure, Room 104, The Deuce, and

Vice Principals; and full scripts and cast lists for the seventh season of the television series Game of Thrones, only two episodes of which had been publicly released by July 23, 2017. The e-mail concluded with the following image, depicting the "Night King," a character from Game of Thrones, and bearing the message, "Good luck to HBO":

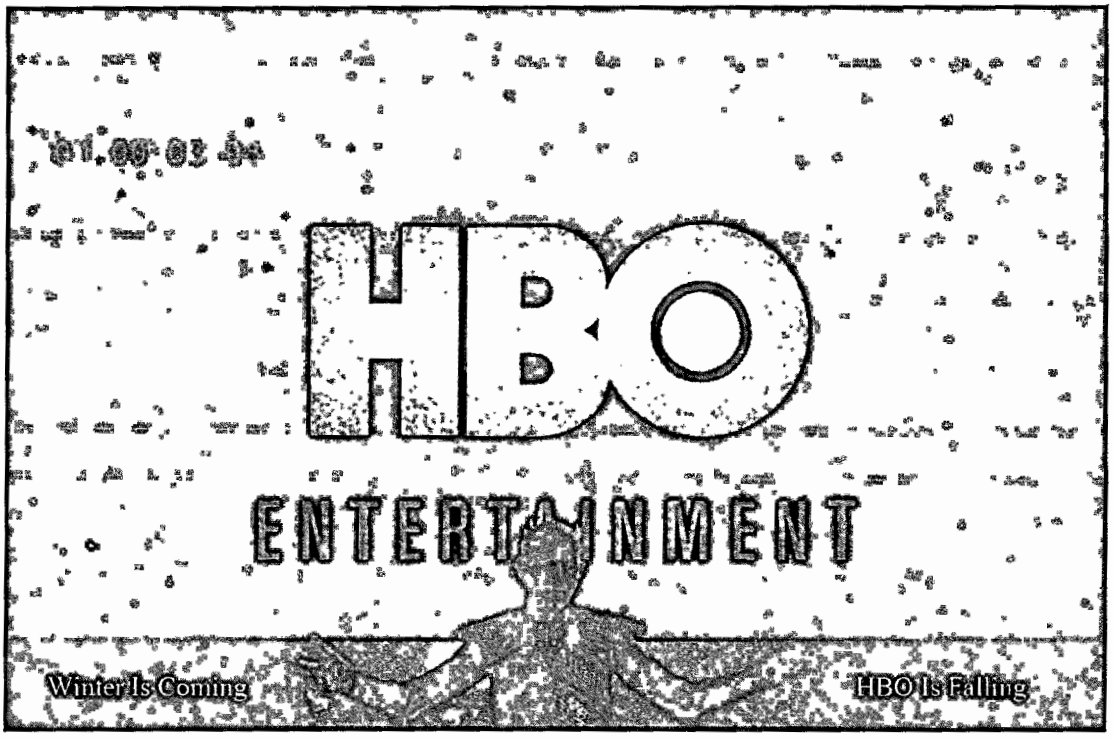


c. On or about July 26, 2017, an anonymous e-mail was sent to HBO personnel that stated, in substance and in part, that the ransom demand had been increased to approximately $6 million dollars' worth of Bitcoin. Further, in addition to repeating threats to publicly release the Stolen Data, the message included threats to destroy data on HBO computer servers, stating, "what about wiping PetaBytes of information [o]n release day? 80 Terabyte hard drives!!!"

d. On or about July 29, 2017, an anonymous e-mail was sent to HBO personnel that included, among other things,

information regarding Bitcoin addresses to which HBO should direct ransom payments, and provided a firm deadline of later that same day for HBO to begin making ransom payments if it wanted to prevent the public leak of the Stolen Data.

7. Starting on or about July 30, 2017, and continuing through at least in or about August 2017, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, caused portions of the Stolen Data to be publicly leaked over the Internet on websites that he controlled. Certain of the video materials that MESRI caused to be leaked included a superimposed graphic depicting the "Night King" image, as depicted in the following video still image taken from the opening credits of an as of then unaired episode of the new HBO series, Barry:



8. BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, undertook efforts to promote the leaks of the Stolen Data on the Internet, including by, among other things, causing e-mails to be sent to members of the media regarding the leaks, and causing the creation of a Twitter profile to announce the leaks and provide evidence of the hack of HBO's computer network.

STATUTORY ALLEGATION

9. From at least in or about May 2017 through at least in or about August 2017, in the Southern District of New York and elsewhere, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, who will be first brought to the Southern District of New York, intentionally accessed a computer without authorization and exceeded authorized access, and thereby obtained information from a protected computer, for purposes of commercial advantage and private financial gain, the value of which information exceeded $5,000, and did aid and abet the same, to wit, MESRI accessed without authorization HBO's computer networks, and stole proprietary data belonging to HBO and transferred the data to computer servers under his control.

(Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B), and 2; Title 18, United States Code, Section 3238.)

COUNT TWO
(Wire Fraud)

The Grand Jury further charges:

10. The allegations contained in paragraphs 1 through 8 of this Indictment are repeated and realleged as if fully set forth herein.

11. From at least in or about May 2017 through at least in or about August 2017, in the Southern District of New York and elsewhere, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, who will be first brought to the Southern District of New York, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, and aided and abetted the same, to wit, MESRI used stolen login credentials of authorized users of HBO's computer network to obtain unauthorized access to that network and to steal proprietary data belonging to HBO.

(Title 18, United States Code, Sections 1343 and 2; Title 18, United States Code, Section 3238.)

COUNT THREE
(Computer Fraud - Threatening to Impair the Confidentiality of Information)

The Grand Jury further charges:

12. The allegations contained in paragraphs 1 through 8 of this Indictment are repeated and realleged as if fully set forth herein.

13. On or about July 23, 2017, in the Southern District of New York and elsewhere, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, knowingly and with intent to extort from a person any money and thing of value, transmitted in interstate and foreign commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and aided and abetted the same, to wit, MERSI caused the transmission of an e-mail to HBO representatives threatening to publicly release confidential and proprietary information belonging to HBO, unless HBO paid a ransom of approximately $5.5 million dollars' worth of Bitcoin.

(Title 18, United States Code, Sections 1030(a)(7) and 2.)

COUNT FOUR
(Computer Fraud - Threatening to Damage a Protected Computer/Impair the Confidentiality of Information)

The Grand Jury further charges:

14. The allegations contained in paragraphs 1 through 8 of this Indictment are repeated and realleged as if fully set forth herein.

15. On or about July 26, 2017, in the Southern District of New York and elsewhere, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, knowingly and with intent to extort from a person any money and thing of value, transmitted in interstate and foreign commerce a communication containing a threat to cause damage to a protected computer and a threat to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and aided and abetted the same, to wit, MESRI caused the transmission of an e-mail to HBO representatives threatening to delete data on HBO's computer network and publicly release confidential and proprietary information belonging to HBO, unless HBO paid a ransom of approximately $6 million dollars' worth of Bitcoin.

(Title 18, United States Code, Sections 1030(a)(7) and 2.)

COUNT FIVE

(Computer Fraud - Threatening to Impair the Confidentiality of Information)

The Grand Jury further charges:

16. The allegations contained in paragraphs 1 through 8 of this Indictment are repeated and realleged as if fully set forth herein.

17. On or about July 29, 2017, in the Southern District of New York and elsewhere, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, knowingly and with intent to extort from a person any money and thing of value, transmitted in interstate and foreign commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and aided and abetted the same, to wit, MESRI caused the transmission of an e-mail to HBO representatives threatening to publicly release confidential and proprietary information belonging to HBO, unless HBO paid a ransom of approximately $6 million dollars' worth of Bitcoin.

(Title 18, United States Code, Sections 1030(a)(7) and 2.)

COUNT SIX

(Interstate Transmission of an Extortionate Communication)

The Grand Jury further charges:

18. The allegations contained in paragraphs 1 through 8 of this Indictment are repeated and realleged as if fully set forth herein.

19. On or about July 26, 2017, in the Southern District of New York and elsewhere, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, knowingly and with intent to extort from a person, firm, association, and corporation, any money and other thing of value, transmitted in interstate and foreign commerce a communication containing a threat to injure the property and reputation of the addressee and of another, and aided and abetted the same, to wit, MESRI caused the transmission of an e-mail to HBO representatives threatening to delete data on HBO's computer network and publicly release confidential and proprietary information belonging to HBO, unless HBO paid a ransom of approximately $6 million dollars' worth of Bitcoin.

(Title 18, United States Code, Sections 875(d) and 2.)

COUNT SEVEN
(Aggravated Identity Theft)

The Grand Jury further charges:

20. The allegations contained in paragraphs 1 through 8 of this Indictment are repeated and realleged as if fully set forth herein.

21. From at least in or about May 2017 through at least in or about August 2017, in the Southern District of New York and elsewhere, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), and aided and abetted the same, to wit, MESRI transferred, possessed, and used, and aided and abetted the transfer, possession, and use of, the usernames and passwords of various employees at HBO during and in relation to the wire fraud and computer fraud offenses charged in Counts One through Five of this Indictment.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b) and 2.)

FORFEITURE ALLEGATION AS TO COUNTS ONE AND THREE THROUGH FIVE

22. As a result of committing one or more of the offenses alleged in Counts One, Three, Four and Five of this Indictment, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real or personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of the offenses alleged in Counts One, Three, Four, and Five of this Indictment, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offenses.

FORFEITURE ALLEGATION AS TO COUNTS TWO AND SIX

23. As a result of committing the offenses alleged in Counts Two and Six of this Indictment, BEHZAD MESRI, a/k/a "Skote Vahshat," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, any and all property, real or personal, which constitutes or is derived from proceeds traceable to the commission of the offenses alleged in Counts Two and Six of this Indictment, including but not limited to a sum of money in United States

currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Assets Provision

24. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Sections 981 and 1030, Title 21, United States Code, Section 853(p), and Title 28, United States Code,

Section 2461, to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981 & 1030;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)

FOREPERSON

JOON H. KIM
Acting United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

BEHZAD MESRI,
a/k/a "Skote Vahshat,"

Defendant.

SEALED INDICTMENT

17 Cr. ___

(18 U.S.C. §§ 875, 1028A, 1030, 1343, 3238 and 2.)

JOON H. KIM
Acting United States Attorney.

TRUE BILL

Kim Johnson
FOREPERSON

11/8/17 - Filed Sealed Indictment
ap
A/W issued.
J P Oetken